Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего профессионального образования

**«Национальный исследовательский ядерный университет «МИФИ»**

**ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ**

**Кафедра №42 (криптологии и кибербезопасности)**

ЛАБОРАТОРНАЯ РАБОТА №2  
по дисциплине: «Системы аналитических вычислений»

**Выполнили:**студенты группы Б19-515  
  
Галацан Никита Георгиевич  
Изъюров Николай Евгеньевич  
Родионов Дмитрий Александрович

**Москва, 2022**

Оглавление

[Построение конечного автомата 3](#_Toc98261319)

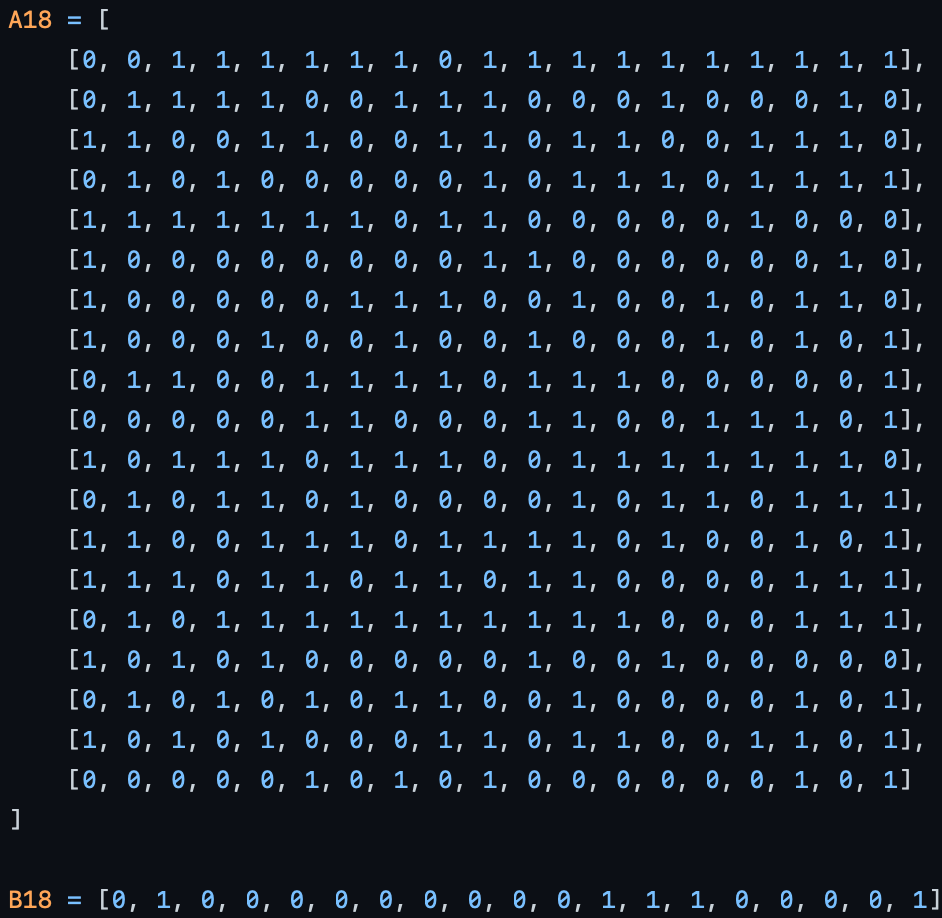
[Нахождение функций де Брейна 5](#_Toc98261320)

[Приложения 7](#_Toc98261321)

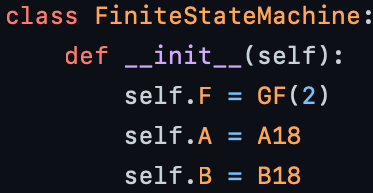
[Заключение 8](#_Toc98261322)

# Построение конечного автомата

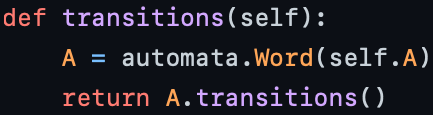
**Вариант №18:**



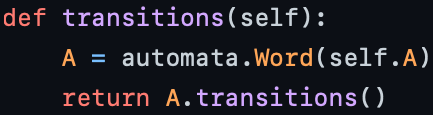
Поставленная задача выполнена с использованием пользовательского класса FiniteStateMachine:



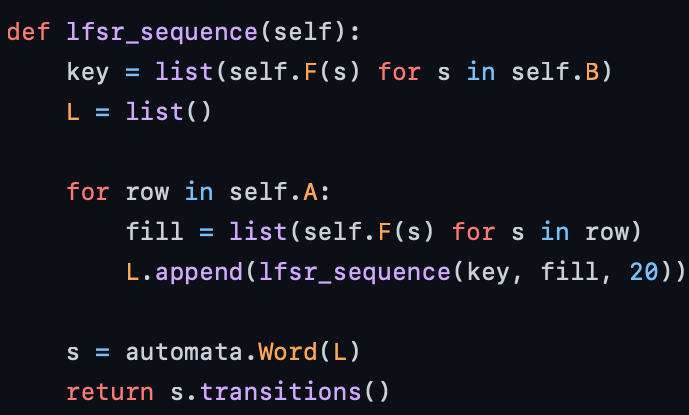
Для создания объекта линейного автомата, соответствующего исходной матрице A, используется встроенный метод Word():



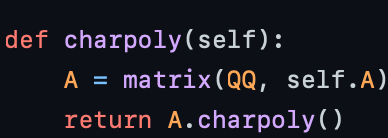
Вывод состояния конечного автомата осуществляется с помощью метода transitions():



Для построения эквивалентного регистра сдвига с линейной обратной связью используется функция lfsr\_sequence():

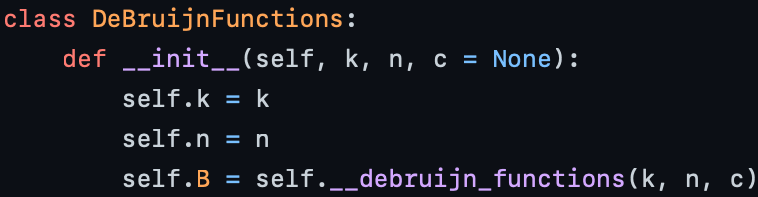


Для вычисления характеристического полинома применяется метод charpoly():

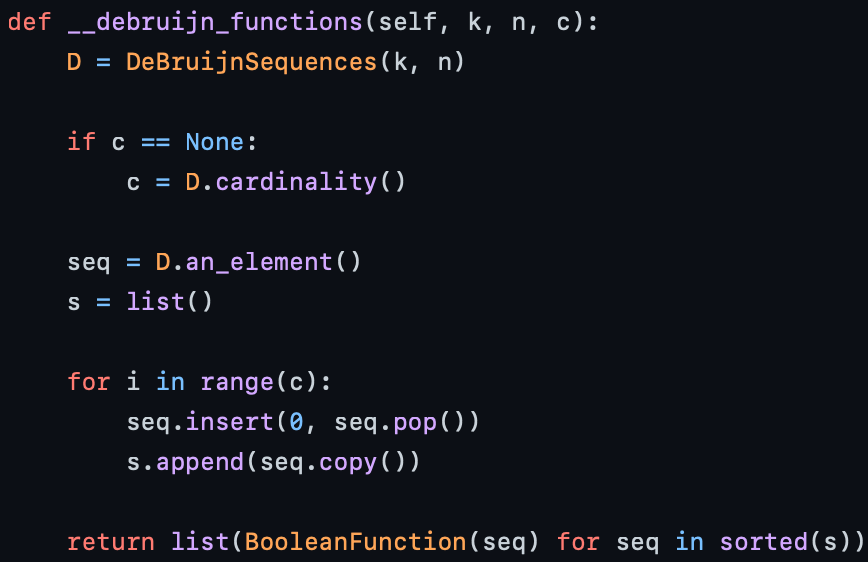


# Нахождение функций де Брейна

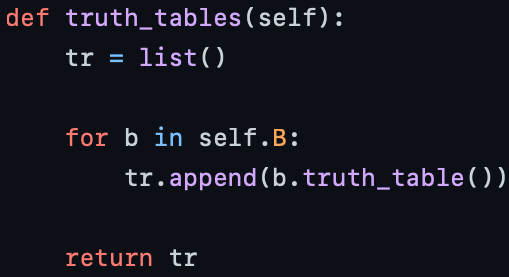
Поставленная задача выполнена с использованием пользовательского класса-обертки DeBruijnFunctions: для обработки функций де Брейна, зависящих от различного числа переменных, используется унифицированный программный интерфейс: конструктор класса принимает опциональный параметр c (*cardinality*), соответствующий количеству рассматриваемых в задаче последовательностей де Брейна:



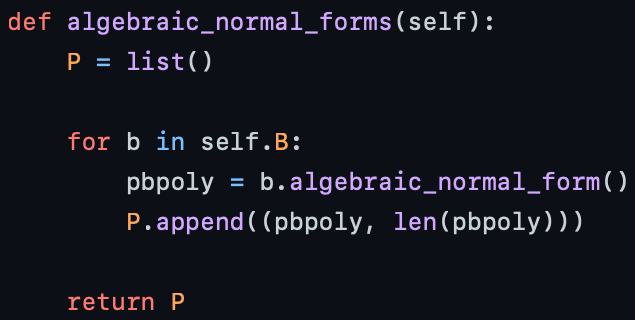
Для инициализации списка булевых функций, соответствующих последовательностям де Брейна, используется метод \_\_debruijn\_functions():



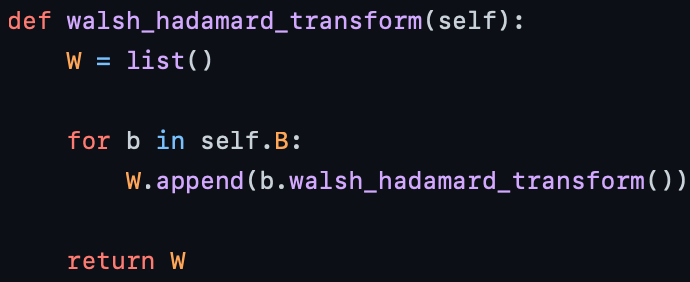
Построение таблиц истинности осуществляется с помощью метода truth\_tables():



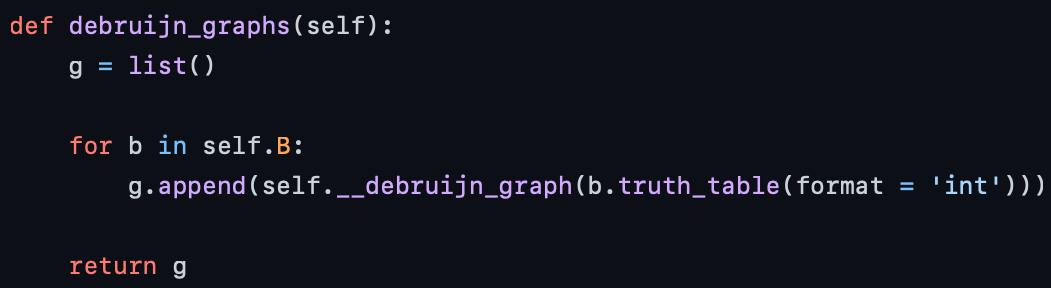
Для вычисления полинома Жегалкина применяется метод algebraic\_normal\_forms():



Расчет коэффициентов Адамара-Уолша производится с использованием метода walsh\_hadamard\_transform():



Нахождение циклов вершин графа осуществляется с помощью метода debruijn\_graphs():



# Приложения

**Листинг функции main:**



# Заключение

В данной лабораторной работе построена математическая модель данных, состоящая из конечного автомата и графа де Брейна.

Для линейного автомата, определяемого матрицей А и вектором В:

* построен эквивалентный регистр сдвига;
* записан рекуррентный закон;
* вычислен характеристический многочлен.

Для каждой функции де Брейна приведены:

* цикл вершин графа;
* таблица истинности;
* полином Жегалкина;
* коэффициенты Адамара-Уолша.

Цель, поставленная в начале работы, достигнута; задачи выполнены.